

29 NASA-TM-X-53563 END
9 (January 6, 1967) 10

1 NASA

GEORGE C. MARSHALL SPACE
FLIGHT
CENTER

HUNTSVILLE, ALABAMA 3

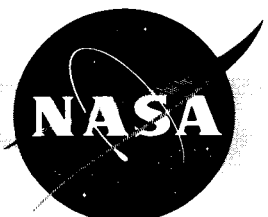
N67-29997
(ACCESSION NUMBER)
103/17
(PAGES)
TMX-53563
(NASA CR OR TMX OR AD NUMBER)

FACILITY FORM 50

(THRU)
1
(CODE)
31
(CATEGORY)

3 SYSTEM SAFETY HANDBOOK 6

National Aeronautics and Space Administration



Rg/45552

APPROVAL


SYSTEM SAFETY HANDBOOK

January 11, 1967

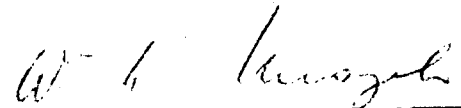
This handbook was prepared by The Boeing Company in accordance with the requirements of Contract NAS8-5608, Schedule II, Part I Exhibit AA, Paragraph 11.5.

25

2901



Preston T. Farish
I-RM-F
Technical Manager
NASA-MSFC



William A. Mrazek
I-DIR
Assistant Director for Engineering
NASA-MSFC

TABLE OF CONTENTS

1.0	INTRODUCTION	1-1
2.0	SCOPE	2-1
3.0	FUNCTIONAL ACTIVITIES	3-1
3.1	GENERAL	3-1
3.2	TEST PARTICIPATION	3-5
3.3	FAILURE ANALYSIS	3-6
3.4	ACCIDENT/INCIDENT INVESTIGATION	3-7
4.0	SYSTEM REQUIREMENTS	4-1
4.1	GENERAL	4-1
4.2	ELECTRICAL	4-3
4.3	PNEUMATIC	4-6
4.4	LIQUIDS	4-10
4.4.1	NON-CRYOGENIC	4-10
4.4.2	CRYOGENIC	4-11
4.5	HYDRAULIC	4-15
4.6	TRANSPORTING AND HANDLING	4-16
4.7	ORDNANCE	4-18

1.0 INTRODUCTION

The testing of a hardware system consists of subjecting it to carefully controlled operating conditions for the purpose of demonstrating that this system performs its function properly.

It follows then, that there is a certain risk inherent in every hardware test program.

The immense size and complexity of major space systems, together with the press of tight schedules have greatly increased this risk.

Reduced to the simplest of terms, there are four essential requirements prerequisite for increasing the probability of a successful test program. These include:

1. The test procedures should be analyzed to ensure that they do not set up conditions that are hazardous to the system.
2. Positive control should be exercised to ensure that deviations from the procedures are limited and that deviations which must be implemented are thoroughly analyzed to ensure that they do not set up a series of events that are out of proper sequence.
3. The desired configuration of the system for each specific test must be known and positive steps should be taken to ensure that the system is in the desired configuration before beginning the test.

4. The test crew should have a thorough understanding of the mechanics of each test and what it is to demonstrate.

There are a great number of detailed requirements which, if adhered to, should greatly reduce the risk associated with testing a system. Many of these requirements have been included in this document. Others will be added as they are identified.

Most of the above comments also apply to maintenance, handling, and operation activities, all of which are included in this document.

2.0 SCOPE

This handbook has been prepared to describe the typical problem areas and equipment within the Saturn System, that experience has shown to require special attention, if hazards are to be avoided or eliminated during test, maintenance and operation.

It is not intended that this handbook levy new design requirements against a well established system; rather the contents are consistent with the present state of the Saturn development, and apply only to the remainder of the program as a guide.

Suggestions for additions to this handbook are welcome and new information will be added as it becomes available.

3.0 FUNCTIONAL ACTIVITIES

3.1 GENERAL

One of the functions of the System Safety Engineer is to determine that certain conditions exist during the performance of the test program or, in the event that he identifies an out-of-tolerance condition, to initiate action as required by his respective management directives. Some of these conditions are listed in the following paragraphs.

3.1.1 Configuration Establishment

The test article should be in a baseline configuration when it is installed in the test stand. There may be additional baselines established as a result of the addition or removal of test hardware. Each test procedure should begin at one of these baselines and should conclude with the restoration of the system to one of these baselines or establishment of a new baseline so that there is a known starting point for the next test.

3.1.2 Procedure Analysis

Test, maintenance, or operating procedures should be analyzed to ensure that none of the steps on the procedure sets up a conflicting or out-of-series event that the system cannot tolerate.

3.1.3 Adequacy of Procedures

All test procedures should be entirely adequate; they should:

- A. Contain system schematics for the test setup in question.
- B. Provide verification blocks.

- C. Include statements of personnel and equipment schematics.
- D. Include caution and warning blocks which provide adequate information, marked in such a way as to minimize the possibility that they will be ignored.
- E. Not require the use of supporting documentation.
- F. Contain an itemized listing by part number, of tools, instruments, and test equipment required to support performance of the test.
- G. Contain requirements for the removal of test equipment installed for performance of tests, i.e., return to basic configuration.

3.1.4 Deviations from Procedures

There should be no deviations from the procedures except those specifically authorized by personnel having the capability and the responsibility for taking such actions; further, any deviations which do occur should be permanently logged.

3.1.5 Overlapping Procedures

Any procedures which may overlap should be integrated into a single procedure such that the overlap is rigidly controlled.

3.1.6 Backout Procedures

Any test leading to conditions which might require emergency or backout procedures should have these procedures properly designed and readily accessible for use at any time during the test without delay.

3.1.7 Test Responsibility

During every test there should be one test conductor who is completely responsible for both the test and the hardware itself, and is readily available to the test crew for advice or decisions.

3.1.8 System Operating Data

Data on all active systems should be recorded during all testing for the purpose of reconstructing the actual test conditions in the event that any accident or incident occurs.

3.1.9 Personnel Certification

Tasks requiring certification should be performed only by currently qualified and certified personnel.

3.1.10 Shift Changes

When practicable, there should be no shift changes during any given test; if shift changes are necessary, they should be controlled by shift overlaps, log entries, and acceptance of the transferred responsibility.

3.1.11 Action for Minimum Hazard

Members of the test crew who are required to make decisions should be indoctrinated with the philosophy of always making their decisions in the direction of minimum hazard.

3.1.12 Safety Checklists

Safety checklists should be included as part of each procedure and should be rigidly adhered to.

3.1.13 Test Stand Communication

Tests requiring intercom-type communications should be minimized and tests which do require this type of equipment should include a checkout of the intercom system as one of the initial steps of the procedure.

3.1.14 Oral Instructions during Testing

Procedures which contain instructions to be given orally during the test which are phonetically similar to other reasonable instructions should explain these instructions in sufficient detail to reduce the probability of wrong action.

3.2 TEST PARTICIPATION

The System Safety Engineer should participate in all major tests on an advisory basis for the purpose of identifying hazards, establishing risk levels and making recommendations for alternative methods. He should be readily available during all testing.

3.3 FAILURE ANALYSIS

The System Safety Engineer should ensure that all component failures are analyzed to determine:

- A. Whether the failure in question could have had a different effect had it happened at some other time during the testing,
- B. Potential impact of such a failure on the safety of the operational system,

and to provide a feedback of test operations to the parent System Safety Organization. He should contribute the maximum amount of support to failure analyses.

3.4 ACCIDENT/INCIDENT INVESTIGATION

The basic purpose of an accident/incident investigation is to consider every possible factor causing or contributing to the accident or incident such that similar occurrences can be prevented in the future. An accident usually results from several contributing events rather than from a single cause. System Safety should be represented on the investigation board. As a board member the System Safety Engineer has the responsibility of influencing the board, insofar as is possible, to consider all possible causes and not overlook any possible contributing factor.

4.0 SYSTEM REQUIREMENTS

4.1 GENERAL

The system requirements listed in this section are those requirements which are applicable to more than one system or which are applicable to systems having no direct association with the vehicular systems.

4.1.1 Interlocks

Interlocks should be provided to preclude concurrent operation of incompatible subsystems within a system or between two separate systems.

4.1.2 Remote Operations

Since computers and switches can and do cause mechanical functions to occur at remote locations, it is imperative for safety that proper interfaces exist between the system in question and (1) other systems, or (2) personnel who might be affected by these mechanical functions. All activities should be integrated with the Test Sequence Order in order to maintain the interface.

4.1.3 Safing of Solenoid Valves

Certain solenoid valves in various systems could readily create a hazard at a remote area if inadvertently activated. These systems are sometimes safed with a manual valve in series with the solenoid valve. When this is done, the initial hazard is removed but there may be another hazard created if the manual valve is not in the proper position at the beginning of a test. Therefore, in these situations, positive control must be established to ensure that the manual valves are in the proper position at the beginning of each test.

4.1.4 Switch Guards

All toggle switches in critical system control panels should be guarded to prevent inadvertent operation.

4.1.5 Safety Valve Validation

No system requiring a pressure regulator, pressure reducing valve, safety valve, or pressure relief valve should be activated unless all assemblies are in place and validated as operable.

4.1.6 Main Power Loss

Any auxiliary power source and switching capability provided to run fire deluge pumps, escape provisions, lighting, hazard detection, and warning systems during an emergency when main power is lost, should be identified and verified as operable before beginning any test series.

4.2 ELECTRICAL

4.2.1 Connector Mismates

Under ideal conditions, all connectors should be sized or keyed such that misconnections are physically impossible. One possible alternate to this is to size the connectors corresponding to their location or function and to key the connectors differently within these groups. In this way either the connectors cannot be mated or temporary mismatching will cause no damage because the types of connectors which can be mismatched are limited. Since this has not been done in the Saturn System, special attention must be given to the proper mating and verification of connectors before power is applied to the system.

4.2.2 Method for Connecting

When connecting operations are being performed, each connector should be inspected to assure they are the proper mates and each connection should be made, disconnected, inspected, and remade to preclude the occurrence of undesired events resulting from bent or otherwise damaged pins.

4.2.3 NIX Contacts

Electrical contact points which could be connected during system test but which never should be connected because their connection will create an unsafe condition should be positively identified by color-coding or other means. (These points are sometimes called NIX contacts.)

4.2.4 Abnormal Contacts

The operation and use of switches, cable connectors, and junctions points should be such as to prevent electrical contacts being made other than those desired for normal system operations.

4.2.5 Switch Activations

Electrical switches which are temporarily deactivated for reasons of safety should be tagged with "Danger" tags or locked out.

4.2.6 Undesired Coupling

Test, operating, and maintenance procedures and test and calibration equipment should not by their use, result in the undesired coupling of electrical energy from one element to another. Items of equipment which are used in conjunction with each other can sometimes cause unexpected fault paths to exist because of the way in which they are connected or used. Equipment and procedures should be examined for these conditions. The avoidance of undesired capacitive and inductive storage and discharge of electrical energy is included in this requirement.

4.2.7 Test Currents

Test equipment supplying test currents should be current-limited to a value such that no actual or potential hazards are created by its use. Failure modes of test equipment should, in all cases, result in a test current less than the non-hazardous test current limit.

4.2.8 Faults to Ground

Special care should be taken to prevent plus fault-to-ground circuits.

4.2.9 Equipment Grounding

Grounding of all hardware (including test and maintenance equipment and ground support and flight hardware) should be provided to prevent the accumulation of hazardous charges and to avoid hazards due to electrical storms.

4.2.10 Phase and Polarity Reversals

During maintenance and installation operations, power phasing should be checked to avoid conditions leading to phase reversals and circuit or polarity reversals.

4.3 PNEUMATIC

4.3.1 Relief Valves

Relief valves set at 110 percent of the system operating pressure should be installed and the use of a valve or other restricting device, either between the pressure and the relief valve or downstream of the relief valve, should be prohibited. Relief valves should be of sufficient capacity to relieve the system faster than the source can pressurize it.

4.3.2 Test Pressure Level

All sources of test pressure should be reduced through pressure regulators to the level to which the test article is to be subjected.

4.3.3 Source Pressure Level

Pressure gauges should be installed in the pressurizing portion of the system such that the source pressure is known at all times. Blocking valves should be placed downstream of critical gauges so that the gauges can be tested and shown to be operable before starting to pressurize the system for the test.

4.3.4 Bleed Valves

Bleed valves should be installed in areas where entrapment of fluid and gases can occur.

4.3.5 Valve Disassembly

Hand valves should be opened halfway prior to disassembly, to vent any trapped pressure.

4.3.6 Valve Consoles

Valve consoles should have a venting capability.

4.3.7 Isolation Valves

Pressure storage tanks installed in the system should have isolation valves to provide independent shutoff capability.

4.3.8 Leak Testing

Leak test crews should not be allowed near the test article until the pressurization process has been completed and the vessel has stabilized for ten minutes.

4.3.9 Tank Damage

Relatively minor damage to tankage such as deep nicks or scratches may cause explosive failure when the tank is pressurized. Small flaws can be progressive depending on metal strain and type of load. Tankage should be protected from and regularly inspected for such damage. If damage is incurred, the system should be thoroughly analyzed for possible effect.

4.3.10 Electrical Interference

All pressure systems should be properly shielded, bonded, and grounded to prevent static electricity and random electrical interference from causing a malfunction. (See Paragraph 4.2.9.)

4.3.11 Pressure Gauge Range

The maximum dial range of test system pressure gauges should be limited to three times the working pressure and the gauge should operate at mid-scale at normal operating pressure.

4.3.12 Pressure Gauge Markings

All single-use gauges should be color-banded to show System Operating Range (green), Marginal Range (yellow), and Hazardous Range (red), or in an equivalent manner.

4.3.13 Pressure Component Proof Testing

Proof tests of equipment should be accomplished at the appropriate proof pressure and certified before running any functional tests at the equipment operating pressure.

4.3.14 Additional Proof Testing of Pressure Components

Any items or components to be installed in pressure systems should be proof-tested and certified as to proof pressure prior to installation both initially and subsequent to modification or repair. This testing should also be accomplished when the system has been:

- A. Subjected to extreme heat or blast effects.
- B. Physically damaged.
- C. Damage is suspected.
- D. Visual inspection indicates excessive corrosion or other deterioration.

4.3.15 Proof Testing Medium

Whenever possible, proof pressure testing should be done hydrostatically.

4.3.16 Proof Testing Precautions

Vessels being subjected to pressures ten percent in excess of the normal operating pressure or higher, should be considered as a type of testing-to-destruction and proper precautions should be taken to protect the surrounding test equipment from possible explosion of the vessel.

4.3.17 High Pressure Flex Lines

The use of high-pressure flexible lines should be avoided, except where absolutely necessary and when used, the hoses should not be longer than required.

4.3.18 Flex Line Protection

The ends of all flex lines should be closed with a bright colored cap or otherwise sealed when not in use.

4.3.19 Connector Mismates

Different types and/or sizes of connections should be used for fuel and oxidizer hoses to prevent inadvertent loading of the wrong system. A special technique should be developed and included as part of the operating procedures in case connectors can be interchanged.

4.4 LIQUIDS

4.4.1 Non-Cryogenic

4.4.1.1 Personnel Indoctrination

The nature, handling characteristics and hazards of liquids should be thoroughly explained to all personnel working within the immediate area.

4.4.1.2 Control Markings

Fuel and oxidizer control displays should be clearly marked with dissimilar color coding and positive provisions made to preclude inadvertent operation of the wrong switch.

4.4.1.3 Electrical Grounding

Prior to initiating any propellant transfer operation, all system components and static grounding cables should first be attached to the vehicle/equipment and then to ground. (See Paragraph 4.2.9.)

4.4.2 Cryogenic

4.4.2.1 Purging

Systems must be purged before the introduction of cryogenic liquids. Purging material must be compatible with the system and the fluid normally used.

4.4.2.2 Purging Medium

Purging of cryogenic systems should be done with helium. If nitrogen is used in a hydrogen system the temperature should be above -320°F to avoid the possible liquification or freezing of the nitrogen.

4.4.2.3 Contaminants

Contaminants must be kept out of cryogenic systems since any contaminants will tend to freeze in the system, clogging, and jamming valves in addition to creating hazardous mixtures during a warm-up period.

4.4.2.4 Materials Compatibility

Any lubricants, seals, thread packing, gaskets or substance which could come into contact with a cryogenic should be compatible.

4.4.2.5 Relief Valves

Relief valves should be installed in any section of a vessel or line where fluid entrapment may occur. Burst diaphragms should be installed in parallel with relief valves.

4.4.2.6 Blocking of Relief Valves

The use of a valve or other restricting device either between the pressure vessel and the relief valve, or downstream of the relief valve should be prohibited.

4.4.2.7 Relief Flow Capability

Relief valves and burst diaphragms should be capable of venting sufficient flow to handle both the maximum input flow and the flow created by temperature rises of the cryogen.

4.4.2.8 Design of Relief Devices

No relief valves or burst diaphragms except those which have been specifically designed to operate at cryogenic temperatures should be used.

4.4.2.9 Fail-Safe Valves

Fail-safe valves should be used. (Fill-fail closed, vent-fail open)

4.4.2.10 Relief Valve Operating Level

Relief valves should be set to operate at 110 percent of the system operating pressure.

4.4.2.11 Burst Diaphragm Operating Level

Burst diaphragms should be set to operate at 120% of the system operating pressure.

4.4.2.12 Relief Valves Functional Check

Relief valves should be checked functionally prior to beginning each test.

4.4.2.13 Vacuum Jacket Relief

Provisions should be made for relieving the vacuum portion of vacuum jacketed containers.

4.4.2.14 Facilities Vents

Vents in buildings housing equipment using hydrogen should be located in the ceiling and should never be closed.

4.4.2.15 Hydrogen Venting

Hydrogen should be vented at low velocity to prevent buildup of static electricity or autoignition. For high volume venting a burn pond with continuous ignition should be used. In vent stacks, flame arrestors should be used.

4.4.2.16 Transfer Line Expansion

Transfer lines should be designed for expansion and contraction through the complete range of temperatures encountered.

4.4.2.17 Condensate on Transfer Lines

Transfer lines which are uninsulated, or with leaking insulation may collect liquid air-oxygen mixtures which can be combustible. The condensate should not be allowed to build.

4.4.2.18 Transfer Line Connections

Connections in cryogenic piping systems whenever possible, should be welded. Quick connects should be avoided. Special welding techniques should be used to prevent oxidation. Any material used to check welds should be compatible with the cryogenic material.

4.4.2.19 Positive Pressure on Containers

Storage tanks and containers should be kept under positive pressure to prevent the infusion of outside contaminants.

4.4.2.20 Electrical Grounding

Cryogenic shipping and storage vessels should be electrically grounded. (See Paragraph 4.2.9.)

4.4.2.21 Electrical Devices

Purged or sealed electrical devices should not be replaced with explosion-proof devices during the course of maintenance. Gas flow should be verified on purged devices and positive pressure should be verified on sealed devices.

4.4.2.22 Insulation Damage

Immediate attention should be given to insulation damage. Over-pressurization can occur with extreme rapidity when there is a heat leak to a stored cryogen. The pressures possible run into the thousands of pounds.

4.4.2.23 Low Temperature Instruments

No instruments should be used except those built especially for use in low temperature applications and marked as such.

4.4.2.24 Portable Testing Equipment

Portable testing equipment must be of a type suitable for use in hazardous gas areas.

4.5 HYDRAULIC

4.5.1 Inactive System

No portion of a hydraulic system should be allowed to remain under pressure when it is inactive unless the system has been specifically designed for such condition.

4.5.2 Preparation for Maintenance

Any system should be depressurized and drained before it is worked on. Particular care must be taken that low points in the system are drained.

4.5.3 Flexible Lines

Flexible lines should be avoided. When they are necessary, they should be as short as possible.

4.5.4 Materials Compatibility

Gaskets, packings, and sealing compounds should be compatible with the hydraulic fluid in the system.

4.5.5 Hydraulic Fluid

Changes in the type of fluid in the system should not be made unless the system is first drained and purged.

4.6 TRANSPORTING AND HANDLING

4.6.1 Handling Procedures

Procedures written for the transportation, protection, and handling methods for any equipment which requires special transportation because of its size or fragile properties, should be reviewed.

4.6.2 Hoisting Procedures

Hoisting procedures for every piece of equipment of unusual weight or size should be reviewed. Centers of gravity should be located and marked so that components will not be overly stressed during handling. The weight should also be stated to enable adequate hoisting equipment to be used.

4.6.3 Hoisting Equipment

Any hoisting or handling equipment (cranes, transporters, slings, pallets, hooks, cables, etc.) must be load-tested to criteria designated by Facilities Engineering at regular intervals. Cables should be inspected for any breaks or signs of weakening.

4.6.4 Makeshift Equipment

No unplanned or makeshift equipment should be used at any time during the loading, packing, or transporting of any items. If the proper equipment or materials are not available, no processing should be done until they become available.

4.6.5 Loading and Unloading

Whenever possible, the same personnel should handle loading and unloading at any location.

4.6.6 Driver Requirements

All vehicles should be operated by drivers who have been tested and certified.

4.6.7 Transportation Routes

Over the road routes for transportation should be studied and pre-selected for maximum safety and minimum accident potential. All tunnels, overpasses, bridges and structures, which could cause damage, must be pre-surveyed for clearances and certified as passable before the route is selected. Hours of travel in some areas may have to be pre-selected to ensure safe transportation for equipment.

4.6.8 Configuration of Transported Articles

All openings on the transported equipment must be covered with seals or plugged to control the internal environment of the stage.

4.7 ORDNANCE

The storage, handling, installation, and use of ordnance items should be in accordance with MSFC Document "Ordnance Systems, Saturn V Launch Vehicle."